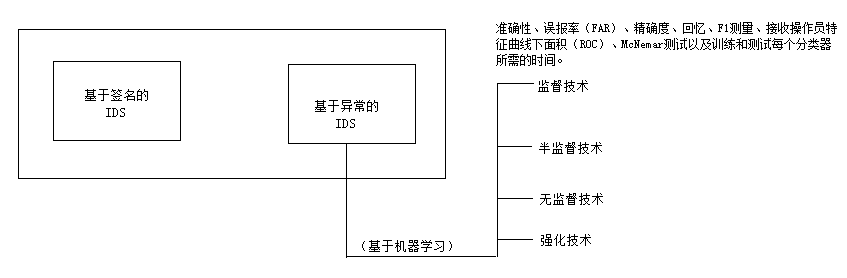
Towards an efficient anomaly-based intrusion detection for software-defined networks

IET Networks

Revised 19th July 2018

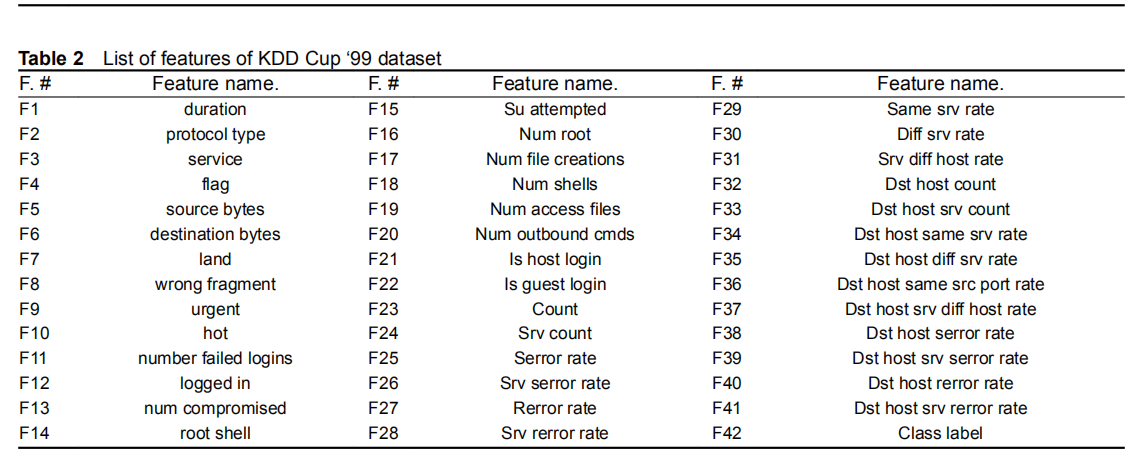
基于异常的IDS可以分为三大类[5]：基于统计的方法、基于知识的方法和基于机器学习的方法。在本研究中，我们主要研究基于机器学习的方法。机器学习技术可分为四大类：（i）监督技术，（i i）半监督技术，（i i i）无监督技术和（iv）强化技术。在本研究中，我们研究了各种监督学习技术，包括其准确性、误报率（FAR）、精确度、回忆、F1测量、接收操作员特征曲线下面积（ROC）、McNemar测试以及训练和测试每个分类器所需的时间。

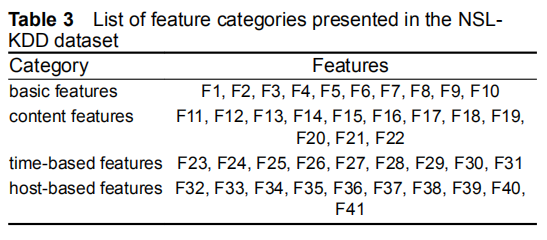


3 数据集：

我们使用了nsl-kdd数据集

kdd cup99和nsl-kdd数据集都包含表2中所示的特性。值得一提的是，这些特性分为四个不同的类别，如表3所述。





如表4所示，NSL-KDD共包括39次攻击，其中每一次都被分为以下四类（DOS、R2L、U2R和Probe）

此外，这些攻击中的一组只在测试集中引入。这些新攻击以粗体显示。

此外，表5显示了NSL-KDD训练和测试集中的正常和攻击记录分布。

4 特征提取

在训练集上应用主成分分析

PCA的标准方法的步骤：

1. 求归一化D维数据集的协方差矩阵。
2. 找出协方差矩阵的特征向量和特征值。
3. 按降序对特征值进行排序。
4. 选择对应于k个最大特征值的k个特征向量。
5. 从k个选择的特征向量构造投影矩阵。
6. 变换原始数据集以获得新的k维特征空间。

在本研究中，我们按以下步骤使用PCA：

1. 首先，我们从主成分中提取具有最大系数的特征。
2. 其次，我们选择对应于k个最大特征值的k个本征向量。
3. 第三，我们使用来自k个选择的特征向量的投影矩阵来变换具有相应特征的原始数据集。
4. 最后，我们通过在训练测试中应用DT方法来验证所选特征和相应k分量的性能。

5 评估指标 ：

根据准确度，FAR，精确度，召回率，F1测量值，ROC曲线下面积[曲线下面积（AUC）]，执行时间和McNemar测试来评估每个分类器的性能。一个好的IDS应该实现高水平的准确性，精确度，召回率和低FAR的F1测量。

(1)准确度



真阳性（TP）是正确分类的攻击记录数；真阴性（TN）是正确分类的正常流量记录数；假阳性（FP）是错误分类的正常流量记录数，假阴性（FN）是错误分类的攻击记录数。

1. FAR



1. 每个分类器的精度



1. 召回率



1. F1度量



1. 执行时间
2. ROC的曲线分析（AUC）
3. McNemar检验

此外，我们还根据执行时间以及ROC曲线的分析来评估先前选择的分类器的性能，其中AUC可用于将每个分类器与另一个分类器进行比较。AUC越高，IDS越好。另一个可用于比较两种算法的重要指标是McNemar检验，这是一种非参数对检验，表明一种算法相对于另一种算法实现了统计上显着的增加。当McNemar检验的z值> 1.96（p <0.05）时，结论是两个算法之间存在显着差异。Z-score用于显示置信水平[20]

6 实验结果

这九个选定的功能是F27，F30，F5，F23，F8，F1，F2，F39和F3。

在表7和表8中，可以观察到与使用SDN控制器（F1，F2，F5，F6，F23和F24）提供的基本特征相比，使用PCA特征选择增强了大多数分类器的准确度水平。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | AUC(ROC) | 精度 | 召回率 | F1-度量 | FAR | Training  time | Test time |
| DT | 0.997 | 83.24% | 96.50% | 89.38% | 3.99% | 0.891s | 0.0257 |
| RF | 0.997 |  |  |  | 3.49% | 2.977s | 0.0674 |
| LogitBoost |  |  | 97.24% |  | 2.83% | 9.158 | 0.1756 |
| AdaBoost |  | 80.23% | 96.65 | 87.67% |  |  |  |
| BaggingTrees | 0.993 |  | 96.56% |  | 3.51% |  |  |
| RUSBoost |  | 77.41% |  | 85.95% |  |  |  |
| ELM | 0.925 | 75.86% | 85.71% | 73.98% | 3.57% | 0.1744 | 0.025 |
| KNN | 0.981 | 82.31% | 96.41% | 82.17% | 3.53% | 12.3421 | 1.9385 |

另一方面，从图4b可以看出ELM方法达到了最佳测试时间。此外，ELM已经实现了可接受的FAR，如表7所示。因此，ELM及其改进的分层方法[22]可能是SDN的有效选择。

尽管KNN方法在测试阶段具有良好的准确性，但它显示出最差的测试时间，这可能表明KNN算法不是SDN的最佳选择，其中每个控制器可能需要 每秒处理数千个流量。通过应用适当的采样方法减少训练实例的数量，可以实现对该问题的可能解决方案。

总结：我们使用PCA方法进行特征选择和降维。使用NSL-KDD数据集并基于我们的实验研究，我们得出结论，DT方法在准确性，精确度，F1测量，AUC和McNemar测试方面表现出最佳性能。与SDN控制器提供的基本功能相比，使用PCA方法非常成功地将准确度从80.31提高到88.74％。